Usare GPG e il client del remailer mixmaster con Mutt

spialaspia@inventati.org

v0.1 10/10/2002

Guida all'integrazione di GPG/PGP e del remailer mixmaster nel client di posta mutt

---

1. Mutt + GPG/PGP

La configurazione necessaria e' ridotta al minimo in quanto con mutt vengono distribuiti 3 files con nome gpg.rc, pgp2.rc e pgp6.rc Se avete usato la versione distribuita come sorgenti (.tar.gz) questi files si trovano nella directory /contrib, e potete copiarli in una cartella del tipo /usr/local/share/mutt/

A questo punto basta scrivere dentro il vostro .muttrc questa riga:

source /usr/local/share/mutt/gpg.rc

se volete usare GPG, oppure pgp2.rc se usate PGP 2.6.3 o pgp6.rc se usate PGP 6.x

Si possono definire alcune variabili nel .muttrc:

per user_ID si intende lo user_ID della vostra chiave pgp che potete visualizzare con

$ gpg --list-secret-keys

e' il nome/indirizzo che compare nella parte piu' a destra dell'output

```
  ------------------------------------------------------------
  (~)% gpg --list-secret-keys
  /home/pinco/.gnupg/secring.gpg
  ------------------------------

  sec  1024R/2EC66601 1995-04-19 pinco@pallino.org
  uid                            putro <pinco@sempronio.com>

  sec  1024D/3DA1AECD 2001-05-24 pinco <pinco@pallino.org>
  ssb  2048g/12A3A4B3 2001-05-24
  ------------------------------------------------------------
```

In questo caso pinco ha 2 chiavi, la prima e' RSA (si riconosce dalla lettera R dopo il numero 1024, mentre la seconda e' DH). Al posto dello userID si possono usare anche i KeyID, ossia il numero che identifica la chiave, nel caso soprastante i keyID sono rispettivamente 2EC66601 e 3DA1AECD, cosi' che se si hanno 2 chiavi con gli stessi UserID si puo' specificare quale usare di default.

Quindi, alcuni dei parametri che si possono modificare sono:

```
set pgp_sign_as=user_ID  (oppure KeyID)
        per definire con quale identita' firmare i messaggi
        (utile se si usa piu' di una chiave)

set pgp_autosign
        per firmare tutti i msg che si scrivono

set pgp_ignore_subkeys
        ignora le subkeys (normalmente non e' importante visualizzarle)

set pgp_replyencrypt
        se un msg e' criptato la nostra risposta sara' criptata

pgp_replysignencrypted
        se un msg e' criptato e firmato la nostra risposta sara' firmata

set pgp_replysign
        se un msg e' firmato la nostra risposta sara' firmata

set pgp_timeout=300
        definisce per quanti secondi la password digitata viene tenuta
        in memoria (default=300)
```

In genere comunque i settaggi di default funzionano piu' che bene per le normali esigenze di un utente, questi comandi assumono invece una certa importanza se usate piu' di una chiave PGP (ossia se avete "personalita' multiple), oppure se avete una gestione dei messaggi criptati basata su folder diversi, o utenti diversi.

Ad esempio se caio@aaa.net usa una PGP 2.6.3 con chiave RSA mentre voi usate GPG con chiave DH ma avete anche una chiave RSA puo' essere molto utile un settaggio di questo tipo:

send-hook caio@aaa.net 'source /usr/local/doc/mutt/samples/pgp2.rc'

send-hook caio@aaa.net 'set pgp_sign_as=0x2EC66601'

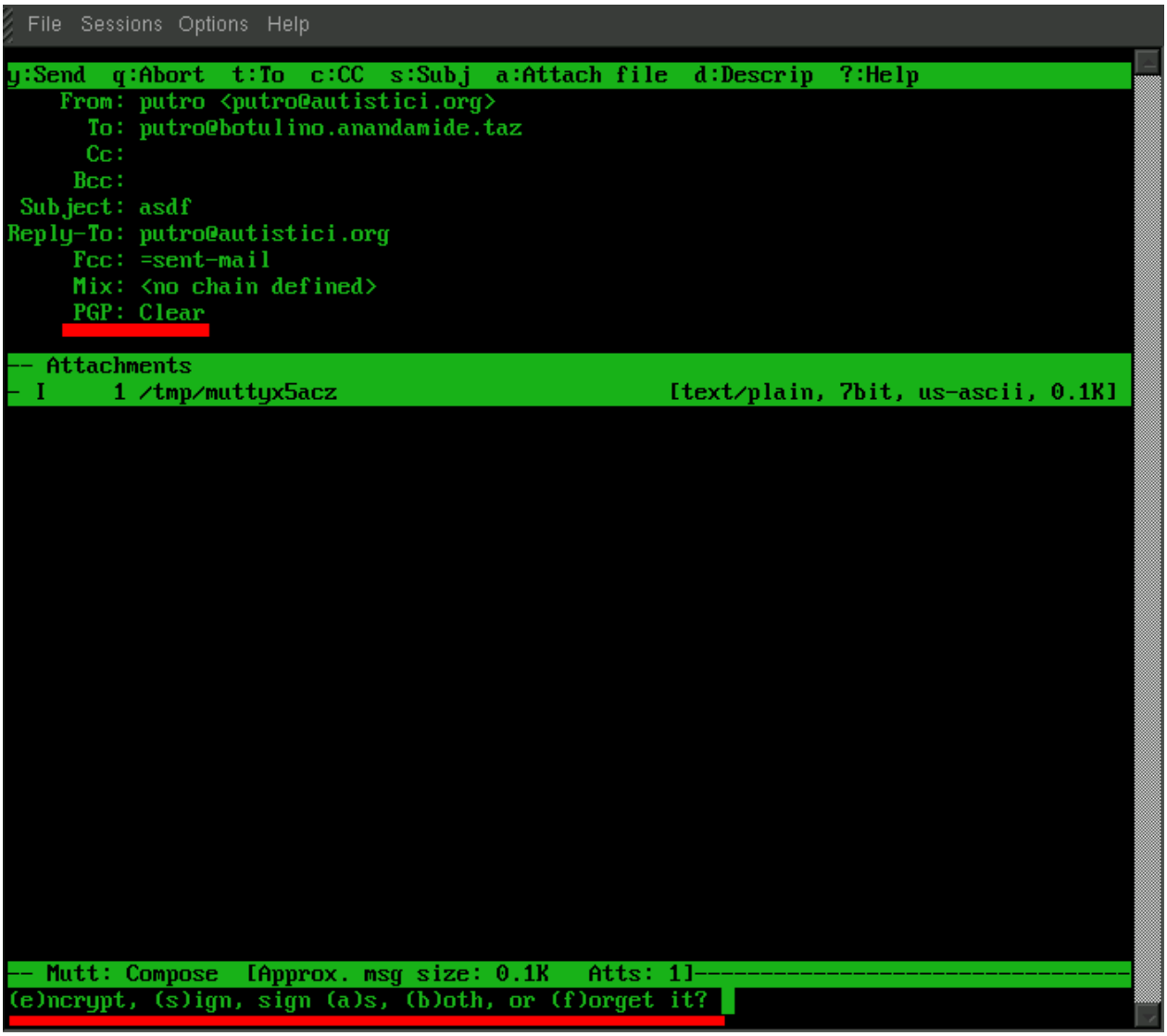
in modo che i messaggi che spedite a caio (e solo quelli) siano firmati con la chiave RSA (keyID=2EC66601 nella tabella vista sopra).

Oppure se volete impostare la crittazione automatica di tutti i messaggi che spedite a tizio@tizio.org:

send-hook tizio@tizio.org 'set pgp_autoencrypt'

Quindi si possono definire dei parametri generali, e poi lavorando con i send-hook e folder-hook andare a personalizzare piu' finemente a seconda delle esigenze.

Quanto all'utilizzo vero e proprio, una volta scritto il vostro messaggio e arrivati alla schermata dove si preme "y" per inviare il messaggio, premendo "p" invece vi compare un menu che vi permette di scegliere tra: s) firmare il messaggio e) criptare il messaggio b) firmare e criptare il messaggio f) cancellare la selezione presente, in modo che il messaggio non sia ne firmato ne criptato.



Decidere se criptare e/o firmare

Nella figura si vede come si presenta la schermata dopo aver premuto "p", si vede lo "stato" del messaggio:

PGP: Clear

che indica che non sara' ne criptato ne firmato, a meno che digitiate una delle lettere del menu che compare nell'ultima riga della schermata.

Una volta definita la vostra scelta, questa comparira' nella riga PGP presente sotto le intestazioni del messaggio. Se vi accorgete che la scelta e' sbagliata potete correggerla premendo di nuovo "p" e poi "f" prima di definire di nuovo una scelta.

A questo punto potete premere "y" per inviare il messaggio. Vi verra' chiesto di specificare quale chiave usare se esistono piu' chiavi e/o sottochiavi, selezionate quella che vi interessa e premete enter.

Se non esiste nel vostro keyring pubblico una chiave con user_ID uguale all'indirizzo del destinatario, vi verra' chiesta quale chiave utilizzare chiedendovi di inserire uno userID da ricercare nel keyring, se non ne inserite nessuno e premete enter vi apparira' la lista di tutte le chiavi presenti nel vostro keyring.

Se la chiave del destinatario non e' presente (neanche con uno user_ID diverso dal suo indirizzo di posta) per quello che credo sia catalogabile come un bug dovrete bloccare mutt con ctrl+c, e il messaggio sara' perso.

Un ultimo utile accorgimento:

Nel file .muttrc e' possibile personalizzare i colori anche di semplici parti di testo, e' quindi comodo inserire 3 righe come queste:

```
color body black brightred "BAD signature"
color body black brightyellow "Can't check signature"
color body black brightgreen "Good signature"
```

Per cui se ricevete un messaggio con una firma non verificata verra' evidenziata in rosso la scritta "BAD signature" che compare in cima al messaggio.

Allo stesso modo sara' visualizzato in giallo l'impossibilita' di controllare una firma perche' non disponiamo della chiave pubblica di chi ha firmato il messaggio.

2. Mutt + il client del remailer mixmaster

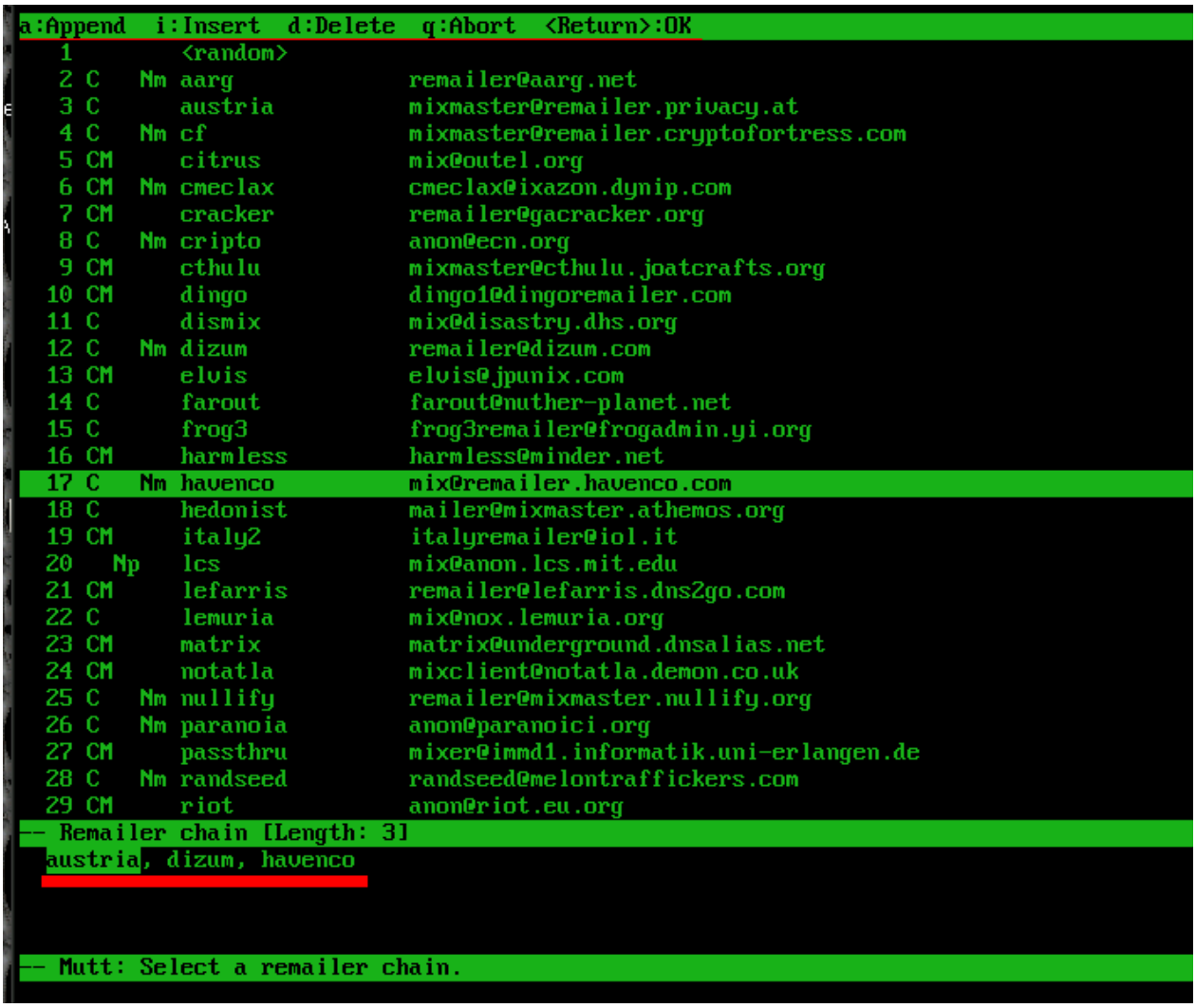
Per poter usare il client del mixmaster mutt deve essere compilato con l'opzione:

$ ./configure --with-mixmaster=path_to_mix

dove path_to_mix e' il path dove si trova il file mix, in genere /Mix In questo modo quando state per inviare il msg e vi trovate di fronte all'ultima schermata (la stessa dove premendo "p" potete criptare e firmare il msg con GPG o PGP), premendo "M" potete scegliere quali remailer usare.

I remailer si selezionano premento lo spazio, oppure "a" o "i" (append e insert), con "d" si cancella il remailer selezionato, e infine con enter si conclude la selezione e si torna alla schermata principale.

Nella figura si vede impostata una catena di 3 remailers: (austria -> dizum -> havenco)



Scegliere la catena di remailer

Se mutt si lamenta del fatto che non avete impostato la variabile hostname, fatelo inserendo nel file .muttrc set hostname=nome.vostro.computer

Ricordatevi di dare il comando

/Mix/mix -S

per spedire i messaggi presenti nel pool quando entrate in rete (ad es. inserendo questa riga in /etc/ppp/ip-up) o inserite il comando nel crontab se il PC ha una connessione permanente.